

## EXPERIMENTAL PERFORMANCE ANALYSIS OF WIRELESS LAN IEEE 802.11N SECURITY MECHANISM

Salman Afsar Awan and Amer Sohail\*

Department of Computer Sciences, University of Agriculture, Faisalabad

\*Corresponding author's e-mail: [sscts104gb@yahoo.com](mailto:sscts104gb@yahoo.com)

A prologue to the topic of Wireless LAN was exhibited so as to provide a survey ahead of the information of a couple Wireless LAN specifications; IEEE (802. 11n) and also IEEE (802.11g). This research was furnished a review of how IEEE (802.11n) and IEEE (802.11g) meets expectations, and in profundity depiction regarding protection issues of both standard was likely displayed, safety techniques accessible, the security defects and what might be carried out with a specific end goal to make a protected WLAN these are all imperative aspects of this research. The conclusion was exhibited that was involved a proposal to utilize IEEE (802.11g) or security strategies.

**Keywords:** WLAN, IEEE802.11n, IEEE802.11g

### INTRODUCTION

A new network which is confided to a number of customers inside a geographical place is termed an area Place Multilevel (LAN) and also a Wi-Fi Neighborhood Multilevel (WLAN) will be the same however with virtually no electrical wires. WLANs tend to be reaching more and more gratitude simply because they can satisfy the growing desire for data from anywhere and also whenever they want. This speedy improvement connected with computing devices and also cellular network strategies has also contributed to its accomplishment. WLAN provide a number of benefits over fixed network like flexibility, range of motion and also scalability (Muller, 2003).

The particular surf can move across walls, entrance doors, over pavement and even straight into different structures. Regardless of whether a gain access to level is found in the place the particular sent files may keep everyone in the room as well as multiply straight into unchecked parts (Theodor, 2000).

WLAN technologies state-of-the-art mobile phone technique as well as Wi-Fi indemnity area time era opening a number of accesses and also program code opening a number of expand entrance to at the similar time(Ahmad, 2007).

While multi-hop transmission from the sender to send more bandwidth to the receiver, it has two major advantage. First An BSS is defined by the distance today. All mobile station which are at the right, but there were restrictions on the distance between the mobile station (Dekleva, 2007).

In 1999, IEEE created IEEE 802. 11b offering some sort of bandwidth involving 11 Mbps, comparable having traditional Ethernet. IEEE 802.11b works by using the same radio signaling regularity (2. 4 GHz) for the reason that first IEEE 802.11 standard. Due to the higher bit rate improve in addition to 802. 11b construed acquire with regard to fast progress (Chen, 2001).

**Types of network:** 802.11 standards define a pair of models: infrastructure mode: a special statement. Improvement involving structure, wireless, composed of daddy, in addition to a minimum of one connected to some sort of wired network structure in addition to wireless station arranged. This kind of construction can be an assistance arranged. In the event the cell station should communicate to the actual satellite structure to a different cell station, the actual connection should be a pair of Leaps. The original mobile station will provide the basis for the access point (AP) (Ergin, 2007).

**IEEE 802.11g:** Typical (IEEE 802. 11g) refer the very best popular features of the two (IEEE 802. 11b) & IEEE 802. 11a along with ended up being brings out in 2003. It supports 54 Mbps bandwidth and operates on 2.4 GHz or greater range. It also has compatibility with (IEEE 802.11b) devices. Higher cost than (IEEE 802.11b) and interference of different appliances are the two drawbacks in this standard.

**IEEE 802.11n:** Up to date IEEE standard (IEEE 802. 11n) is designed to swap this (IEEE 802. 11a), (IEEE 802. 11b) in addition to (IEEE 802. 11g) Wi-Fi standard for LAN. It was created to boost about (IEEE 802. 11g) throughout the volume of bandwidth supported through the use of multiple wireless signals in addition to antennas named MIMO engineering (Multiple Inputs, Several Outputs) rather than a single.

**802.11 Wireless Local Area Network Bandwidth:** Study of IEEE 802.11 operation time under different assumptions of the analysis carried out independently of the geometric form packages, etc. these results also shows standards IEEE 802.11 7.27 Mbit / theory it is possible to lower rates compared to the leg. Intervention was replaced in its simple form, a network wireless networking, and physical wiring

trough radio signals. Unlike cable, radio signals, physical and electromagnetic interference are prone to a variety. The overall capacity of the intervention itself is shown as a decrease, and sometimes completely out of the result (Hara, 2005).

## MATERIALS AND METHODS

To examine the network traffic initially the throughputs were calculated and then the response times were examined. For this function traffic and throughput analyzing tools were utilized to ways a significant research. When the entire research process was regarding to absolute, it was very compulsory to convey the outcomes in an efficient method. All the outcomes were described in graphical way so that everybody can simply realize the outcomes and winding up. For this function Statistics Calculation Tools were used. Before getting started, it is essential to depict the hardware and software requirements used for the research work. According the obligation of the work to be completed it is attractive good to cite the equipment used, in aspects. Hardware and software used throughout the research work is listed under unconnectedly.

**Hardware specifications:** Here is the catalog of hardware utilized in the entire research process.

**Access points:** This research work was comprises of safety contrast of two dissimilar wireless LAN principles IEEE (802.11g) and IEEE (802.11n). So, there were clearly desired two access points supporting these WLAN standards.

- D-Link DWL-2100AP
- D-Link DAP-1353

**Laptops:** Keeping the portability aspect in mind two laptops of the similar merchant were used in its place of desktop computers. Their requirements are as beneath

- HP 2510p
- HP 6910p
- D-Link DWA-645

**Wireless network adapters:** To get precise and accurate results the preference was given to choose Wireless Network Adapters of the same vendor and specification.

- D-Link DWL-G650
- D-Link DWA-645

**Software specifications:** Here is the list of software used in the entire research process whether the operating system or any other traffic examined tool

**Operating systems:** Inside the research process similar operating system was used on mutually machines, Microsoft Windows 7.

Operating system normalized beside with manages with your computer hardware one of several frequent demand programs for the frequent users. Computer learning resource

allocator is able to along with allocates sources. A software program which works as an intermediary between some sorts of end user of your personal computer plus the computers. Captivating out end client programs beside with fashion commerce with end user problems much easier. Manufacture your personal computer system suitable to use. Use the computers inside a creative method (Silberschatz and Gagne, 2006).

**Traffic analyzing tool:** The two kinds of traffic and throughput examined tools were used to perform a significant research.

**Iperf:** Iperf Server Command for TCP Transmission:  
C:\iperf>iperf -s -D -n 10M -w 1K (-w 1K to 1000K & -n 5 MB to 20MB)

Iperf Client Command for TCP Transmission:  
C:\iperf>iperf -c IP Address -n 10M -w 1K (-w 1K to 1000 K & -n 5MB to 20MB)

Iperf Server Command for UDP Transmission:  
C:\iperf>iperf -s -D -n 10M -w 500K -u -l 1 (-l 1K to 1000 K & -n 5MB to 20MB)

Iperf Client Command for UDP Transmission:  
C:\iperf>iperf -c IP Address -n 10M -w 500K -u -b 54M -l 1 (-l 1K to 1000K & -n 5MB to 20MB)

**Ping:** Ping is Windows supports rule to verify the network status of a meticulous machine beside with other information. It was used to verify the connectivity of two laptops with each other and access point.

**DU Meter:** DU Meter is a small data sniffer tool that gives a pictorial/graphical view of data at the time of transmission.

**Statistics calculation tools:** When the entire research process was about to complete, it was very essential to express the outcomes in a regular technique. This is SPSS 13.0 for Windows.

**Security methodology:** There were two broader categories on which whole the research process based:

- Implementing security mechanisms on IEEE 802.11g supporting access point.
- Implementing security mechanisms on IEEE 802.11n supporting access point.

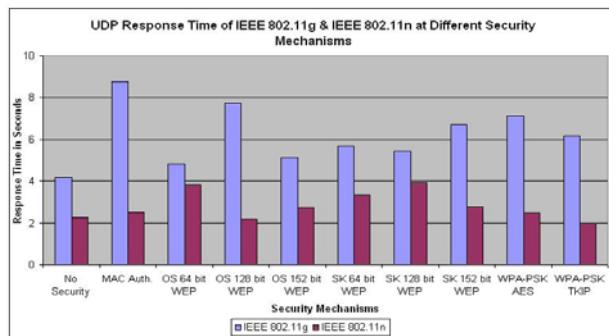
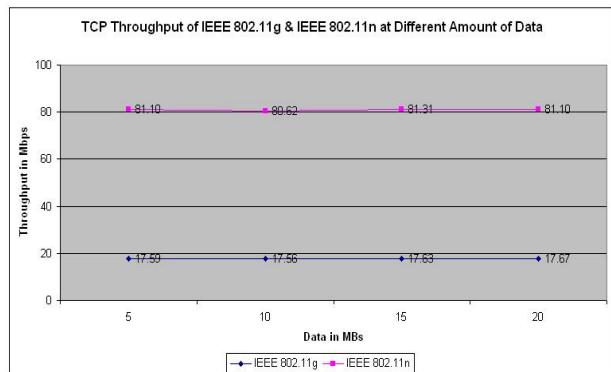
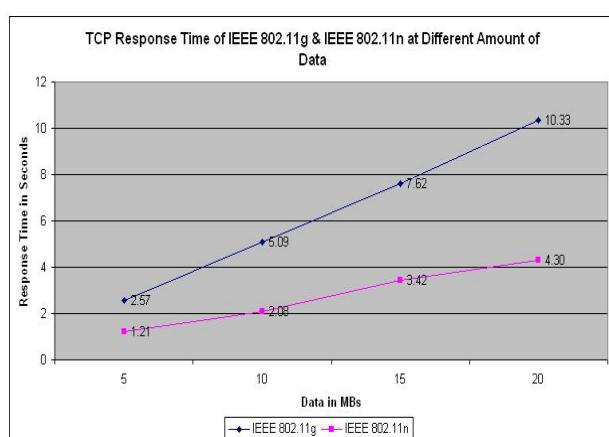
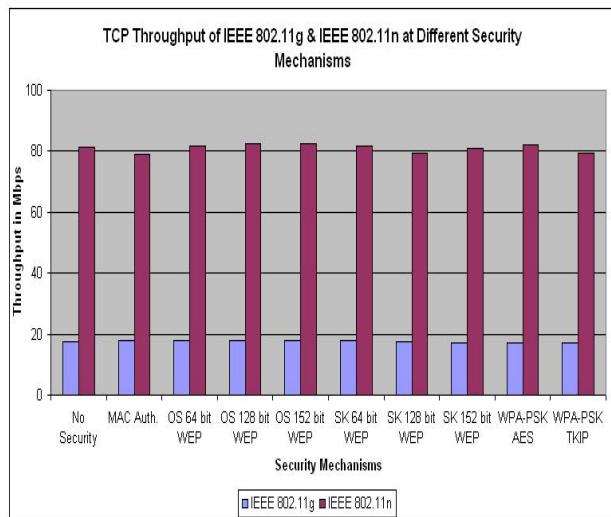
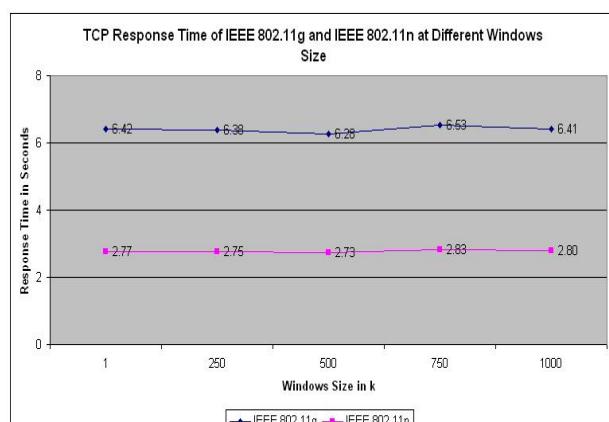
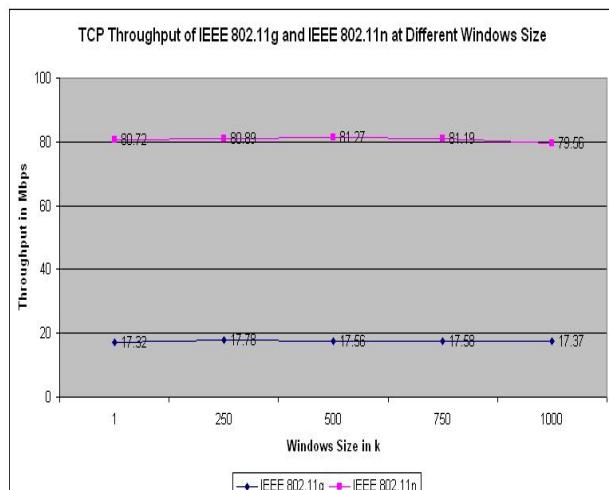
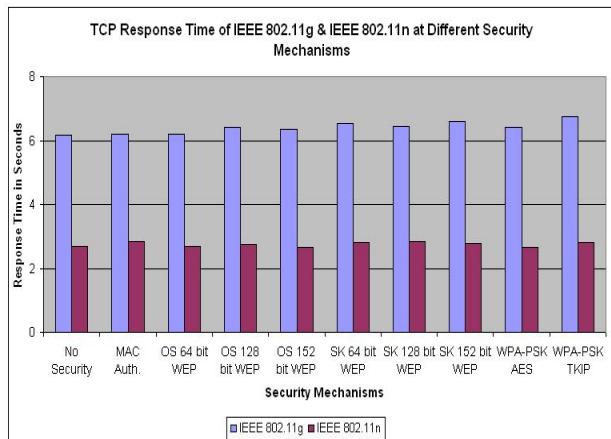
**Security mechanisms:** Only the frequent mechanisms in both WLAN standards were under reflection. The security mechanisms are listed below

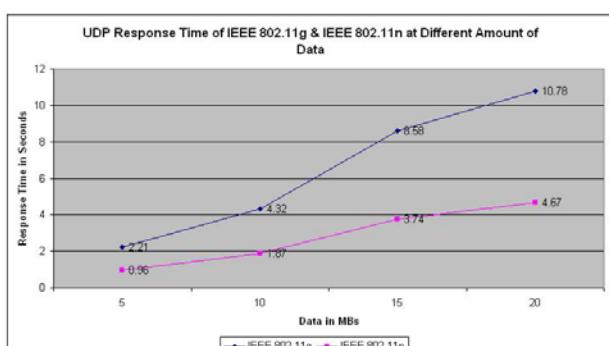
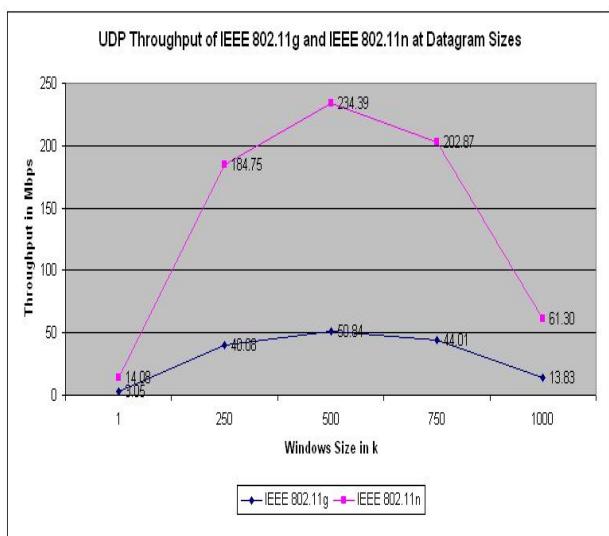
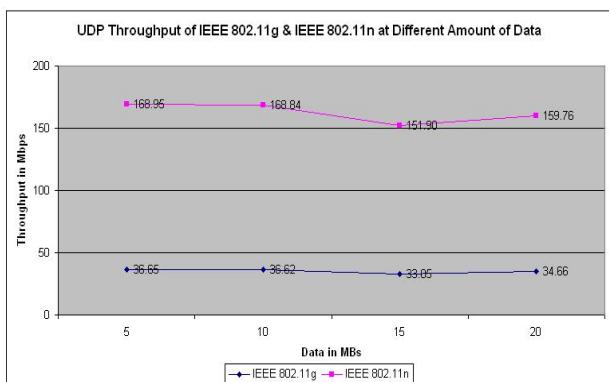
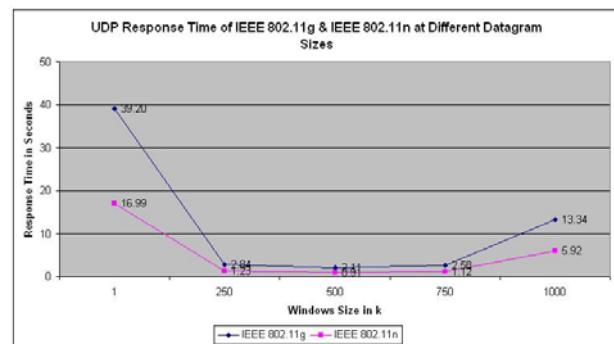
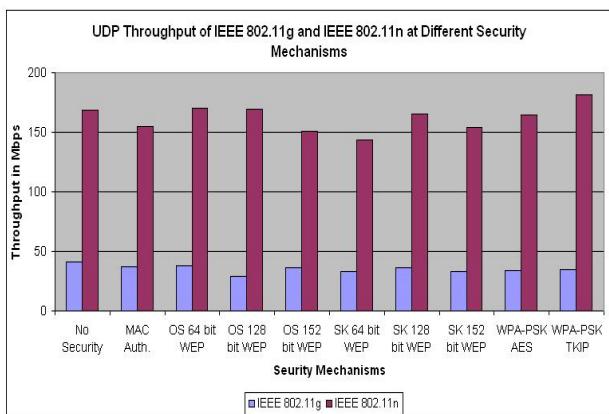
## RESULTS AND DISCUSSION

The key plan of the research is to locate out which WLAN standard IEEE (802.11g) or IEEE (802.11n) provides finest safety mechanisms in conditions of performance.

**Table 1: Security mechanisms applied**

Sr. No.	Security mechanism applied
1	No Security
2	MAC Address Authentication
3	Open System Authentication with 64 bit WEP Encryption
4	Open System Authentication with 128 bit WEP Encryption
5	Open System Authentication with 152 bit WEP Encryption
6	Shared Key Authentication with 64 bit WEP Encryption
7	Shared Key Authentication with 128 bit WEP Encryption
8	Shared Key Authentication with 152 bit WEP Encryption
9	WPA-PSK Authentication with AES Encryption
10	WPA-PSK Authentication with TKIP Encryption





**IEEE 802.11g TCP & IEEE 802.11n TCP analysis:** This is a vital section of results and conversation which mainly focal point on comparing TCP transmission in mutually WLAN standards IEEE 802.11g and IEEE 802.11n.

In above graph TCP response time at dissimilar safety methods illustrates a very flat chart in mutually Wireless LAN standards, IEEE 802.11g and IEEE 802.11n. So as to means there is no attractive alter in time exhausted at any safety stage.

At this point is throughput graph for mutually standards at every security applied? Like TCP response time TCP throughput graph explain that there is no variation diagrammatically and safeties does not influence the throughput in TCP.

This Graph shows TCP throughput at dissimilar quantity of data in IEEE 802.11g and IEEE 802.11n. There is no abnormality in the graph of together standards. Throughput in IEEE 802.11g is additional than 4 times less than IEEE 802.11n.

TCP throughput of IEEE 802.11g and IEEE 802.11n beneath dissimilar windows sizes (1 k, 250 k, 500 k, 750 k and 1000 k) is exposed in line graph. It can be pragmatic in the graph that throughput in mutually the standards is in a very flat way. But IEEE 802.11g throughput is even extra than 4 times less than IEEE 802.11n.

At this point TCP response time is signified in a line graph at mutually WLAN standards beneath the similar windows size as shown in figure 4.40. Though the response time of IEEE 802.11g is additional than twice as evaluated with IEEE 802.11n.

This graph shows the TCP response time in IEEE 802.11g and IEEE 802.11n at dissimilar quantity of data. The enlargement ratio in response time is set to an exacting stage in mutually WLAN standards.

**IEEE 802.11g UDP & IEEE 802.11n UDP analysis:** At this point unequal graph for mutually standards demonstrate that response time in IEEE 802.11g is sensibly greater to IEEE 802.11n. Maximum response time of 9 seconds in IEEE 802.11g was pragmatic at MAC Authentication.

UDP throughout in IEEE 802.11n standard observed minimum 4 times superior than IEEE 802.11g. Approximately, at every safety stages IEEE 802.11n throughput is more than 150 Mbps.

At this point line above graph shows UDP through put at dissimilar quantity of data in together Wireless LAN standards. IEEE 802.11n throughput stick to the bottom line

and average throughput is exposed at every data quantity. At 5 and 10 MB of data, UDP throughput is relatively superior. In figure UDP throughputs are offered at dissimilar datagram sizes (1 k, 250 k, 500 k, 750 k and 1000 k) in 2 WLAN standards (IEEE 802.11g and IEEE 802.11n). On datagram size of 1 k, UDP throughput in mutually standards is very short while by rising datagram size 250 k throughput significantly amplified. While datagram size was kept 500 k, highest throughput was pragmatic in mutually standards. In the ending at 750 k and 1000 k datagram sizes reduces in the similar way as it was amplified. This graph shows the UDP response time between diverse quantities of data in 2 WLAN standards. Here is a sharp growth in response time at mutually standards. It takes extra time to broadcast similar quantity of data in IEEE 802.11g standard as contrasted to IEEE 802.11n.

At this point UDP response time is computed at diverse datagram sizes in mutually WLAN standards (IEEE 802.11g and IEEE 802.11n) as exposed in figure 4. 48. Response time has been pragmatic at its maximum stage through datagram size of 1 k while at 250 k, 500 k and 750 k response time was sensibly short. While at datagram size of 1000 k response time boosts once more.

## **CONCLUSION**

Hence applying much type of securities mechanism in several trial and experimental scenarios, conduct of IEEE (802. 11g) WLAN standard displays a clear losing off through put in addition to increasing response time period because the security level becomes more tricky and tricky. On the other hand under the same experimental setup there isn't almost any importance alters inside throughput or response time in IEEE (802. 11n). However, IEEE (802. 11g) expressed supplementary steadiness inside throughput and also response time as compared to IEEE (802. 11n).

Because received results and also discussion posts show that will throughput and also response time is pretty affected by utilizing security mechanisms inside IEEE (802. 11g) rather than IEEE (802. 11n). It could be concluded that WLAN standard IEEE (802. 11n) provides best security mechanism in comparison together with IEEE (802. 11g).

## **REFERENCES**

Ergin, M.K. Ramachandran and M. Grutest. 2007. Understanding the effect of access point density on wireless LAN Performance, International Conference on Mobile Computing and Networking Proceeding of the 13<sup>th</sup> annual ACM international conference on mobile computing and networking. pp: 62-64.

Hara, O., J. Bob, and S. Petrick. 2005. Al. IEEE 802.11 Handbook: A Designer's Companion(2<sup>nd</sup> ed.). IEEE Press, New York, NY, pp: 241-260.

Muller, J.N. 2003. Wi-Fi for the Enterprise. McGraw-Hill: New York.

Silberschatz, A., P.B. Galvin and G. Gagne. 2006. Operating System Concepts, Windows XP update. Wiley.com.

Theodore, S. 2000. Wireless Communication: Principles and Practice (2nd Edition). IEEE. 17: 60-150.

Ahmad, S. 2007. Exploring the requirements for QoS in Mobile Ad hoc Network. J. Info. Comm. Tech. 1: 45-47.

Dekleva, S., J.P. Shim, U. Varshney and G. Knoerzer. 2007. "Assessing the widespread deployment and increasing use of mobile services. Evolution and Emerging Issues in Mobile Wireless Networks". Communications of The ACM. 50: 38-43.

Chen, J.C. 2001. Measurement Performance of 5-GHz 802. 11a Wireless LAN Systems. Atheros Communication, Inc.